NAME

timingsafe_bcmp, **timingsafe_memcmp** - timing-safe byte sequence comparisons

SYNOPSIS

#include <string.h>

int
timingsafe_bcmp(*const void *b1, const void *b2, size_t len*);

int
timingsafe_memcmp(*const void *b1, const void *b2, size_t len*);

DESCRIPTION

The **timingsafe_bcmp**() and **timingsafe_memcmp**() functions lexicographically compare the first *len* bytes (each interpreted as an *unsigned char*) pointed to by *b1* and *b2*.

Additionally, their running times are independent of the byte sequences compared, making them safe to use for comparing secret values such as cryptographic MACs. In contrast, bcmp(3) and memcmp(3) may short-circuit after finding the first differing byte.

RETURN VALUES

The **timingsafe_bcmp**() function returns 0 or not zero if the byte sequence pointed to by *b1* compares equal to or not equal to (respectively) the byte sequence pointed to by *b2*.

The **timingsafe_memcmp**() function returns a negative value, 0, or positive value if the byte sequence pointed to by *b1* compares less than, equal to, or greater than (respectively) the byte sequence pointed to by *b2*.

SEE ALSO

bcmp(3), memcmp(3)

STANDARDS

The **timingsafe_bcmp**() and **timingsafe_memcmp**() functions are FreeBSD extensions.

HISTORY

The **timingsafe_bcmp**() function first appeared in OpenBSD 4.9.

The **timingsafe_memcmp**() function first appeared in OpenBSD 5.6.

Both functions first appeared in FreeBSD 12.0.